UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/938,790	08/24/2001	Alexander I. Alten	Alten-00100	2157

7590 08/09/2005

Rich Butt
Valley Oak Law
5655 Silver Creek Valley Rd # 106
San Jose, CA 95138

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 08/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/938,790	ALTEN, ALEXANDER I.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) *1-12 and 24-29* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *13-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20020307, 20030502*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Applicant's election without traverse of Invention II, Claims 13-23, in the reply filed on 18 July 2005 is acknowledged.

2. Claims 1-12 and 24-29 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to nonelected inventions, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on 18 July 2005.

Specification

3. The disclosure is objected to because of the following informalities:

The specification appears to contain minor errors. For example, on page 14, lines 10-11, in the sentence "Note that random materials, be it Pads or Keys, ultimately comes from the Server", it appears that "materials" is intended to read "material". Also, on page 17, line 17, it appears that a reference to a set of three Mixing Keys 1624 is intended to refer to a set of Keys 1524.

Appropriate correction is required. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors.

Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Objections

4. Claims 16 and 21 are objected to because of the following informalities: It appears that "accordingt" in each claim is intended to read "according". Appropriate correction is required.

5. Applicant is advised that should claims 13, 14, and 16-18 be found allowable, claims 19-23 will be objected to under 37 CFR 1.75 as being substantial duplicates thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k). The Examiner notes that it appears that Claim 19 is intended to read "A method for deciphering a sequence of cipher text" in place of "A method for enciphering a sequence of cipher text". The objection would be overcome if such a change were made.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 13-23 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 13 and 19 each recite the limitation "the plurality of randomly rotated and large random pads". There is insufficient antecedent basis for this limitation in the claims, although it appears that this is intended to refer to the previously recited "plurality of rotated large random pads". Further, Claims 13 and 19 also recite the limitation "the plurality of rotated and randomly shuffled large random pads"; it appears that this is intended to refer to the previously recited "plurality of randomly rotated and randomly shuffled large random pads".

Claims 14 and 20 each recite the limitation "the plurality of nested shuffled large random secrets". There is insufficient antecedent basis for this limitation in the claims, although it appears that this is intended to refer to the "plurality of shuffled large random secrets" of Claims 13 and 19.

Claims 17, 18, 22, and 23 each recite the limitation "the plurality of random secrets". It is not clear whether this refers to the plurality of large random secrets or the plurality of shuffled large random secrets recited in Claims 13 and 19. This renders the claims indefinite. Further, Claims 17, 18, 22, and 23 also each recite the limitation "the plurality of substitution keys". There is insufficient antecedent basis for this limitation in the claims.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 103

8. Claims 13, 16, 19, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koopman, Jr., US Patent 5696828, in view of Wilson et al, US Patent 5295188.

In reference to Claim 13, Koopman discloses a method for enciphering that includes shuffling a plurality of large random secrets using a plurality of mixing keys (column 5, line 60-column 6, line 22), performing an XOR to produce a plurality of pads (column 7, lines 22-33), rotating the values of the plurality of pads (column 8, lines 18-34, noting the use of a shift register), shuffling a portion of the rotated pads (column 5, line 60-column 6, line 22), performing an XOR to produce a final pad (column 7, lines 22-33), selecting a portion of the final pad to form a key stream (column 7, lines 46-49, where portions of the random numbers are eliminated), and performing an XOR on the key stream and clear text values (column 1, lines 51-58, noting that the generated random numbers are used as a key for a Vernam stream cipher). However, Koopman does not explicitly disclose that the first shuffle is a nested shuffle.

Wilson discloses that random sequences can be used to generate cryptographic keys (column 5, lines 24-30), and that for greater security, shuffling of key material can be done at multiple levels (column 9, lines 26-31, where a global shuffle and a local shuffle can be performed). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Koopman by

29) and provide verifiable random number sequences (see Wilson, column 2, lines 66-68).

Claim 19 is directed to a method of deciphering cipher text that corresponds to the enciphering method of Claim 13, and is rejected by a similar rationale.

In reference to Claims 16 and 21, Koopman further discloses selecting a series of portions to form the key stream (column 7, lines 46-49).

9. Claims 14, 15, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koopman and Wilson as applied to claims 13 and 19 above, and further in view of Ritter, US Patent 5623549.

Koopman and Wilson disclose everything as applied above to Claims 13 and 19; however, neither Koopman nor Wilson explicitly discloses substituting values within the plurality of secrets. Ritter discloses a cipher method that includes initializing mechanisms by substituting values within tables for other values within the tables (column 18, lines 13-18). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the methods of Koopman and Wilson to include the substitution of Ritter, in order to increase the strength of the ciphering (see Ritter, column 5, line 67-column 6, line 2).

10. Claims 17, 18, 22, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koopman and Wilson as applied to claims 13 and 19 above, and further in view of Schneier, *Applied Cryptography*.

In reference to Claims 17 and 22, Koopman and Wilson disclose everything as applied to Claims 13 and 19 above. Wilson further discloses the use of a secure channel for distributing keys (column 1, lines 44-47). However, neither Koopman nor Wilson explicitly discloses the use of a central server to distribute keying information. Schneier discloses that a central trusted server can be used to generate and distribute key information (page 47, "Key Exchange with Symmetric Cryptography", noting the Key Distribution Center). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the methods of Koopman and Wilson by including a Key Distribution Center, in order to gain the security of the trusted secure server (see Schneier, page 47, last paragraph).

In reference to Claims 18 and 23, Koopman and Wilson disclose everything as applied to Claims 13 and 19 above. Wilson further discloses the use of a secure channel for distributing keys (column 1, lines 44-47). However, neither Koopman nor Wilson explicitly discloses the use of a storage medium to distribute keying information. Schneier discloses that the large amounts of key bits for a one-time pad can be distributed on a CD or digital tape (see the paragraph spanning pages 16-17). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the methods of Koopman and Wilson by including distribution of keying information on a storage medium, in order to allow for easy storage and access to the large number of key bits required for a Vernam stream cipher, i.e. one time pad (see Schneier, paragraph spanning pages 16-17).

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Ritter, US Patent 5727062, discloses a cipher system that can include rotations, substitutions, and shuffles.

b. Glover, US Patent 6868495, discloses a system for one time pad encryption key distribution including a shuffling function.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER